UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/721,713	11/27/2000	Jae-han Park	Q61823	4060

7590 05/08/2006

SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037-3202

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 05/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/721,713	PARK, JAE-HAN	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. No claim has been amended in an amendment filed on 4/11/2006. Presently, pending claims are 1 – 14.

Response to Arguments

2. Applicant's arguments with respect to the subject matter of the instant claims have been fully considered but are not persuasive.

3. As to Applicant's assertion that is referred to Office action dated January 27, 2005, Examiner respectfully responds that the argument has no relevance since the submission of RCE starts the new prosecution process dated June 27, 2005 and the proper reference of corresponding Office action on the record should be dated as January 11, 2006.

4. As per claim 1, Applicant asserts: "the Examiner is apparently utilizing impermissible hindsight reasoning, as the Examiner appears to be picking and choosing different portions of the applied reference to satisfy the specific features set forth in claim 1 because the Bluetooth reference does not satisfy at least operations (c) and (d) of claim 1". Examiner respectfully disagrees. The timing sequences of the messages as recited in claim 1 (c) and (d) are disclosed in the Bluetooth reference in the same manner even though they are presented from different portions of the applied reference. The reason can be summarized as follows:

- Bluetooth reference discloses "When the authentication is finished the link key must be created (Page 197, Section 3.3.4)" – i.e. the link key creation is considered as the integral procedure of a successful authentication.
- Bluetooth reference discloses "For mutual authentication, after unit A has successfully authenticated unit B, unit B could authenticate unit A by sending a AU_RAND_B (different from the AU_RAND_A that unit A issued) to unit A, and deriving the SRES and SRES' from the new $AU\_ RAND_B$, the address of unit A, and the link key (Page 170, Section 14.4 and Figure 14.10)" – i.e. unit B can request to authenticate unit A after the successful authentication of unit B by unit A.
- Bluetooth reference discloses "Mutual authentication is achieved by performing first the authentication procedure in one direction and, if successful, immediately followed by performing the authentication procedure in the reversed direction (Page 154, Section 14.2.2.2)".

5. As per claim 7, Applicant argues claim limitation 7(b). Examiner notes please refer to the same rationale set forth above in claim 1.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

6. Claims 1 – 14 are rejected under 35 U.S.C. 102(a) as being anticipated by Bluetooth (Specification of the Bluetooth System Version 1.0 A, July 26th 1999), hereinafter referred to as Bluetooth.

As per claim 1, Bluetooth teaches an authentication method for establishing a connection between devices that can wirelessly communicate data, the method comprising the steps of:

(a) sending a first authentication-request message to another device to perform an authentication procedure with the other device to which a connection is wanted (Bluetooth: see for example, PART C, Section 3.2 Authentication page 194 and Section 3.3 Pairing page 196: first authentication-request message crresponding to LMP_in_rand (or LMP_au_rand) message);

(b) sending a predetermined message according to a current operation mode to the other device and storing the predetermined message when an authentication-response message to the first authentication-request message is received (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key, page 197 & PART C Section 3.3.4, Page 198, Bullets 1 – 3: Examiner notes the reasonable and broadest claim interpretations are made to meet the claim languages as follows: (i) "a predetermined message" corresponding to LMP_unit_key (or LMP_comb_key) message, (ii) "according to a current operation mode" is interpreted as the IF bullet sections described in Page 198, Bullets 1 – 3, (iii) "storing the predetermined message" is interpreted as equivalent to serve the same purpose as

store a value associated with a received key can be retained, which is used in determining the selection of link key (i.e. either LMP_unit_key or LMP_comb_key);

(c) after performing the step (b), checking whether a received first message is a response message corresponding to the predetermined message when the first message from the other device is received (See the same rationale addressed above in (b) – i.e. "a received first message" and "a predetermined message" corresponding to the diffrenet combination of LMP_unit_key (or LMP_comb_key) message. Besides, Bluetooth reference discloses "When the authentication is finished the link key must be created (Page 197, Section 3.3.4)" – i.e. the link key creation is considered as the integral procedure of a successful authentication);

(d) sending a response message corresponding to a second authentication-request message to the other device when the result of checking in the step (c) indicates that the first message is the second authentication request message (Bluetooth: see for example, PART B, Section 14.4 Authentication 4th Paragraph, page 170: Unit B could authenticate unit A by sending a AU_RAND_B according to mutual authentication procedure as taught by Bluetooth. On this subject matter, Bluetooth reference discloses "For mutual authentication, after unit A has successfully authenticated unit B, unit B could authenticate unit A by sending a AU_RAND_B (different from the AU_RAND_A that unit A issued) to unit A, and deriving the SRES and SRES' from the new AU_RAND_B, the address of unit A, and the link key (Page 170, Section 14.4 and Figure 14.10)" – i.e. unit B can request to authenticate unit A after the successful authentication of unit B by unit A. Besides, Bluetooth reference discloses

"Mutual authentication is achieved by performing first the authentication procedure in one direction and, if successful, immediately followed by performing the authentication procedure in the reversed direction (Page 154, Section 14.2.2.2)";

(e) after performing the step (d), checking whether a second message is a response message corresponding to the predetermined message when the second message from the other device is received (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key, Line 1 – 8 & Bullets 1 – 3); and

(f) finishing the authentication procedure when the result of checking in the step (e) indicates that the second message is a response message corresponding to the predetermined message (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key, Line 1 – 16 & Bullets 1 – 3).

As per claim 2 and 6, Bluetooth teaches in the step (b), when the current operation mode is a pairing process, a message for generating a link key is sent as the predetermined message and stored (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key, Line 6 – 16), and when the current operation mode is not a pairing process, a message of connection-establishment-completion is sent as the predetermined message and stored (Bluetooth: see for example, PART C, Section 4 Connection Establishment,3rd Paragraph); and the step (f) further comprises the sub-steps of:

(f1) generating a link key before finishing the authentication procedure when the current operation mode is a pairing process (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key, Line 6 – 16); and

(f2) finishing the authentication procedure and establishing a connection to the other device when the current operation mode is not a pairing process (Bluetooth: see for example, PART C, Section 4 Connection Establishment,3rd Paragraph and Figure 4.1).

As per claim 3, Bluetooth teaches the step (b) further comprises the sub-steps of:

(b1) checking whether the authentication-response message is valid using key information and random information (Bluetooth: see for example, PART C, Section 3.2 Authentication and Section 3.2.1); and

(b2) processing an authentication failure when the result of checking in the step (bl) indicates that the authentication-response message is not valid (Bluetooth: see for example, PART C, Section 3.2.1).

As per claim 4, Bluetooth teaches in the step (b1), the key information is held by the present device and the random information was used in sending the first authentication message (Bluetooth: see for example, PART C, Section 3.2 Authentication).

As per claim 5, Bluetooth teaches (g) finishing the authentication procedure when the result of checking in the step (c) indicates that the received first message is a response message corresponding to the predetermined message (Bluetooth: see for example, PART C, Section 4 Connection Establishment, 3rd Paragraph and Figure 4.1).

As per claim 7, Bluetooth teaches an authentication method for establishing a connection between devices that can wirelessly communicate data, the method comprising the steps of:

(a) sending a response message corresponding to a first authentication request message when the first authentication-request message from another device that wants to establish a connection is received (Bluetooth: see for example, PART C, Section 3.2 Authentication and Section 3.3.1 & Section 3.3.2, Sequence 3 / 4);

(b) after performing the step (a), and prior to performing the step (c), checking an authentication condition of the present device when a predetermined message from the other device is received (Bluetooth: see for example, PART B, Section 14.4 Authentication 4th Paragraph, page 170 & PART B, Section 14.2.2.2 Authentication 2nd Paragraph, page 154: Unit B could also authenticate unit A by sending a AU_RAND_B according to mutual authentication procedure as taught by Bluetooth. Examiner notes please refer to claim 1(c) and claim 1(d) for more details);

(c) after performing the step (b), storing the predetermined message and sending a second authentication-request message to the other device when the result of checking indicates that a mutual authentication is required (Bluetooth: see for example,

PART B, Section 14.2.2.2 Authentication 2nd Paragraph, page 154 & Figure 14.11 and PART B, Section 14.4 Authentication 4th Paragraph, page 170 & PART C, Section 3.3, Sequence 4. Regarding "storing the predetermined message", see the same rationale addressed above);

(d) after performing the step (c), sending a response message corresponding to the message stored in the step (c) to the other device when a response message from the other device corresponding to the second authentication-request message is received, and finishing the authentication procedure (Bluetooth: see for example, PART C, Section 4 Connection Establishment,3rd Paragraph and Figure 4.1).

As per claim 8, Bluetooth teaches in the step (d), when the predetermined message received in the step (b) is a message for generating a link key, the present device sends a response message corresponding to the message for generating a link key to the other device, generates a link key, and then finishes the authentication procedure (Bluetooth: see for example, PART C, Section 3.3.4 Creation of the Link Key, Line 6 – 16 and Sequence 7); and when the predetermined message received in the step (b) is a message of connection-establishment-completion, the present device sends a response message corresponding to the message of connection-establishment completion to the other device, finishes the authentication procedure, and then establishes a connection to the other device (Bluetooth: see for example, PART C, Section 4 Connection Establishment, 3rd Paragraph and Figure 4.1).

As per claim 9, Bluetooth teaches the step (d) further comprises the sub-steps of:

(d1) checking whether the response message corresponding to the second authentication-request message is valid when the response message corresponding to the second authentication-request message is received by using random information and key information (Bluetooth: see for example, Figure 14.11 and PART B, Section 14.4 Authentication 4th Paragraph, page 170); and

(d2) processing an authentication failure when the result of checking in the step (dl) indicates that the response message is not valid (Bluetooth: see for example, PART C, Section 4 Connection Establishment, 3rd Paragraph and Figure 4.1).

As per claim 10, Bluetooth teaches in the step (dl), the present device holds the key information and the random information was used in sending the first authentication message (Bluetooth: see for example, PART C, Section 3.2 Authentication).

As per claim 11 and 14, Bluetooth teaches in the step (b) authentication enable information is checked as the authentication condition (Bluetooth: see for example, PART B, Section 14.4 Authentication 4th Paragraph, page 170: Unit B could authenticate unit A by sending a AU_RAND_B according to mutual authentication procedure as taught by Bluetooth).

As per claim 12, Bluetooth teaches determining whether an authentication procedure for establishing a connection between devices that want to communicate data is performed as a unilateral authentication procedure or as a mutual authentication

procedure, according to an authentication condition which enables receiving an authentication request in the two devices that can communicate data; and performing the authentication procedure (Bluetooth: see for example, PART B, Section 14.4 Authentication 3rd Paragraph, page 170: Examiner notes Bluetooth is relied upon determining whether an authentication procedure for establishing a connection between devices that want to communicate data is performed as a unilateral authentication procedure or as a mutual authentication procedure (Bluetooth: PART B, Section 14.4 Authentication 3rd Paragraph, page 170) - Bluetooth teaches the Link Manager (LM) coordinates the indicated authentication preferences by the application (one-way authentication or mutual authentications) to determine in which direction(s) the authentication(s) has/have to take place by allowing device B to authenticate device A by sending a AU_RAND_B (different from the AU_RAND_A that device A just issued to meet the claim language that recites the procedure based on an authentication condition which enables receiving an authentication request in the two devices . Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993)).

As per claim 13, Bluetooth teaches performing the authentication procedure, when the authentication condition of the device that receives the authentication request is set to require the mutual authentication procedure, the mutual authentication procedure is performed by sending an authentication request message to the device

that requests an authentication (Bluetooth: see for example, Figure 14.11 and PART B, Section 14.4 Authentication 4th Paragraph, page 170).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC

CHRISTOPHER REVAK
PRIMARY EXAMINER

5/4/06